



Docket No.:Ref. 1405.1049

Japanese Laid-open Application Publication No. 11-212849 (D4)

The invention of D4 relates to the shared file transmission and reception system provided with the access control function. ([0001])

The invention of D4 makes the list that describes conditions of a user to allow the access as the conditional equation combined with the attribute information of the user, and stores the shared file added this in the server information processor. It is constructed to acquire the login information of the user who tries to access to it by the client information processor, and based on the list added to the shared file to be accessed, judge the access right by the access right discrimination processor, and send the shared file from the server information processor to the client information processor according to this discrimination. (Abstract)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-212849

(43) 公開日 平成11年(1999) 8月6日

(51) Int.Cl.<sup>6</sup>

G 0 6 F 12/00

識別記号

5 3 7

F I

G 0 6 F 12/00

5 3 7 A

審査請求 未請求 請求項の数20 O L (全 21 頁)

(21) 出願番号 特願平10-16280

(22) 出願日 平成10年(1998) 1月29日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(71) 出願人 000153524

株式会社日立情報ネットワーク

東京都品川区南大井六丁目26番3号

(72) 発明者 鍛 忠司

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 荒井 正人

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 弁理士 富田 和子

最終頁に続く

(54) 【発明の名称】 共有ファイル送受信システム、アクセス権利判定装置

(57) 【要約】

【課題】 共有ファイルへのアクセス権の設定を、ファイルサーバに依らず共通の処理で、かつ、ファイルサーバにおけるアクセス権利設定のための特権を要求することなく行う。

【解決手段】 アクセスを許可するユーザーの条件を、ユーザーの属性情報を組み合わせた条件式として記述したリストが付加された共有ファイルをサーバ情報処理装置11に格納し、アクセスしようとするユーザーのログイン情報をクライアント情報処理装置12で取得し、前記ユーザーのログイン情報およびアクセスしようとする共有ファイルに付加されたリストに基づいてアクセス権利判定処理装置14によりアクセス権利を判定し、この判定に従って共有ファイルを、サーバ情報処理装置11からクライアント情報処理装置12にデータ中継装置13により中継する。

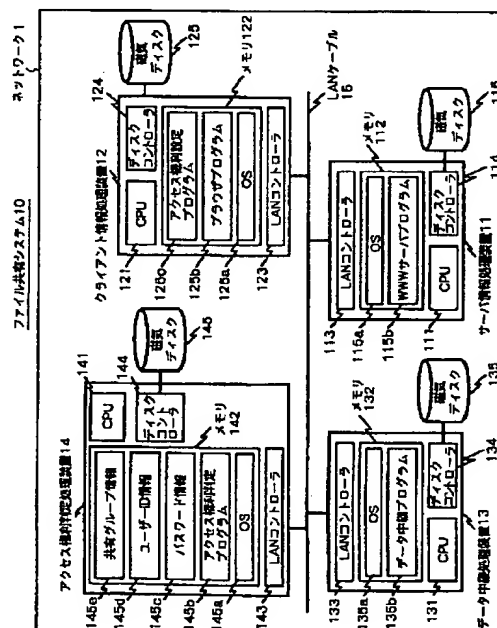


図1

## 【特許請求の範囲】

【請求項1】通信回線を介して接続される端末間で共有ファイルを送受するための共有ファイル送受信システムであって、

共有ファイルにアクセスする権利をデータ受信側の利用者が有するか否かを判定するためのアクセス権利判定手段と、

データ送信側の端末からデータ受信側の端末にファイルを転送するためのデータ中継手段とを備え、

前記共有ファイルは、アクセス権利を持つ利用者を示す開示先情報が予め付加され、

前記アクセス権利判定手段は、共有ファイルにアクセスする権利をデータ受信側の利用者が持つか否かを、当該共有ファイルに付加されている前記開示先情報に基づいて判定し、

前記データ中継手段は、前記データ受信側の利用者の要求に応じてデータ送信側の端末から共有ファイルを受信し、当該受信した共有ファイルに対するアクセス権利を前記利用者が有すると前記アクセス権利判定手段が判定した場合にのみ、前記受信した共有ファイルをデータ受信側の端末に送信することを特徴とする共有ファイル送受信システム。

【請求項2】請求項1記載の共有ファイル送受信システムにおいて、

前記開示先情報は、それが付加されている共有ファイルに対してアクセスが許可される条件が、個人に関する予め定められた属性情報を指定するリストとして記述され、

前記アクセス権利判定手段は、データ受信側の前記利用者に関する属性情報が前記リストの条件を満足する場合に、前記共有ファイルにアクセスする権利があるものと判断することを特徴とする共有ファイル送受信システム。

【請求項3】請求項2記載の共有ファイル送受信システムにおいて、

前記リストは、当該リストを識別するための名称が予め定められ、

前記共有ファイルは、前記リストに代えて、当該リストを示す名称が付加され、

前記アクセス権利判定手段は、前記リストと当該リストの名称との組を保持して、

前記名称に対応する前記リストの条件を前記利用者に関する属性情報が満足する場合に、前記共有ファイルにアクセスする権利があると判断するものであることを特徴とする共有ファイル送受信システム。

【請求項4】請求項2および3のいずれか一項記載の共有ファイル送受信システムにおいて、

前記共有ファイルには、前記利用者がアクセス権利を持たないことを通知するメッセージが付加されていて、

前記データ中継手段は、前記利用者が前記共有ファイル

に対してアクセスする権利を持たないことが、前記アクセス権利判定手段により判断された場合、データ受信側の前記端末に、前記利用者がアクセス権利を持たないことを通知するメッセージを送信することを特徴とする共有ファイル送受信システム。

【請求項5】請求項4記載の共有ファイル送受信システムにおいて、

前記利用者がアクセスする権利を持たないことを通知するメッセージは、データ送信側の前記端末にエラーメッセージファイルとして格納されていて、

前記共有ファイルには、前記メッセージに代えて前記エラーメッセージファイルを示すリンク情報が付加されていて、

前記データ中継手段は、前記利用者が前記共有ファイルに対してアクセスする権利を持たないことが、前記アクセス権利判定手段により判断された場合、データ送信側の前記端末から前記エラーメッセージファイルを受信し、データ受信側の前記端末に前記エラーメッセージファイルを送信することを特徴とする共有ファイル送受信システム。

【請求項6】通信回線を介して接続される端末間で共有ファイルを送受するための共有ファイル送受信システムであって、

アクセスする権利を判定するためのアクセス権利判定装置と、データ受信側の前記端末に前記データを送信するデータ中継装置とが通信回線を介して接続され、

前記アクセス権利判定装置は、

前記共有ファイルに付加された、アクセスする権利を持つ利用者の条件を、個人に関する予め定められた属性情報が組み合わされて記述されたリストを基に、データ受信側の前記端末の利用者が前記共有ファイルにアクセスする権利を持つか否かを判定し、

前記データ中継装置は、

データ送信側の端末から前記共有ファイルを受信し、当該共有ファイルに付加されている前記リストを前記アクセス権利判定装置に送信し、前記利用者に当該共有ファイルに対するアクセス権利があると前記アクセス権利判定装置が判定した場合にのみ、データ受信側の前記端末に前記データを送信することを特徴とする共有ファイル送受信システム。

【請求項7】共有ファイルを格納するための機能、および、転送要求を受けた共有ファイルを転送するための機能を有するサーバ装置と、

前記サーバ装置から共有ファイルを受信するための機能、および、ユーザーに共有ファイルの情報を表示するための機能を有するクライアント装置と、

共有ファイルの転送要求を前記クライアント装置から前記サーバ装置に中継し、共有ファイルを前記サーバ装置から前記クライアント装置に中継するための機能、および、当該共有ファイルをキャッシュするためのキャッシ

機能有する代理サーバ装置と、  
前記共有ファイルに付加された、アクセスする権利を持つ利用者の条件を、個人に関する予め定められた属性情報が組み合わされた記述されたリストを基に、前記クライアント装置の利用者が前記共有ファイルにアクセスする権利を持つか否かを判定するためのアクセス権利判定装置と、

前記サーバ装置から前記共有ファイルを受信し、当該共有ファイルに付加されている前記リストを前記アクセス権利判定装置に送信し、前記アクセス権利判定装置が前記利用者に当該共有ファイルに対するアクセス権利があると判定した場合にのみ、前記代理サーバ装置に前記データを送信するデータ中継装置とが通信回線を介して接続されていることを特徴とする共有ファイル送受信システム。

【請求項 8】通信回線を介して受信した情報を基に、共有ファイルに対するアクセス権利を持つか否かを判断するアクセス権利判定装置であって、  
通信回線を介して受信する前記情報は、アクセスを許可する利用者の条件を、個人の属性情報を組み合わせて条件式として記述したリストであって、  
アクセス権利を持つか否かの判断を依頼した依頼者を特定するための依頼者認証手段と、  
当該アクセス権利判定装置が管理する前記依頼者の属性情報が前記リストを満足する場合には、アクセスする権利を持つと判断するためのアクセス権利判定手段とを備えることを特徴とするアクセス権利判定装置。

【請求項 9】請求項 8 記載のアクセス権利判定装置において、  
アクセスを許可する利用者の条件を記述したリストと当該リストの名称との組を記録するための手段と、  
前記リストの名称から前記リストを検索するための手段とを備え、

通信回線を介して受信される前記リストには、前記共有リストの名称が含まれ、  
前記アクセス権利判定手段は、前記共有リストに前記依頼者に関する情報が含まれている場合にも、アクセスする権利を持つと判断することを特徴とするアクセス権利判定装置。

【請求項 10】通信回線を介して受信した情報を基に、共有ファイルに対するアクセス権利を持つか否かを判断するアクセス権利判定装置であって、  
通信回線を介して受信する情報とは、前記依頼者の属性情報を、暗号鍵と呼ばれる情報によって暗号化したものと、アクセスを許可する利用者の条件を、個人の属性情報を組み合わせて条件式として記述したリストとであって、  
当該アクセス権利判定装置は、前記暗号化された属性情報を、前記依頼者が当該アクセス権利判定装置に登録した、復号鍵と呼ばれる情報によって復号する属性情報復

号手段を備え、

前記アクセス権利判定手段は、前記属性情報復号手段によって復号化した、前記依頼者の属性情報が前記リストを満足する場合には、アクセスする権利を持つと判断するものであることを特徴とするアクセス権利判定装置。

【請求項 11】請求項 8、9 および 10 のいずれか一項記載のアクセス権利判定装置において、

前記依頼者認証手段は、ログイン証明書と呼ばれる情報を受信することによって依頼者を特定するものであり、  
当該アクセス権利判定装置は、前記ログイン証明書を発行する証明書発行手段を備えることを特徴とするアクセス権利判定装置。

【請求項 12】請求項 11 記載のアクセス権利判定装置において、

前記ログイン証明書には、前記依頼者の識別子と、当該ログイン証明書が有効か否かを調べるための情報と、が記録されていて、

当該アクセス権利判定装置は、受信した前記ログイン証明書が有効か否かを調べる有効性確認手段を備え、

前記依頼者認証手段は、前記ログイン証明書が前記有効性確認手段によって有効であると判断された場合には、前記依頼者の識別子によって依頼者を特定するものであることを特徴とするアクセス権利判定装置。

【請求項 13】請求項 12 記載のアクセス権利判定装置において、

受信したログイン証明書を保存するためのログイン証明書保存手段を備え、

前記有効性確認手段は、新たに受信したログイン証明書が、既に保存されている場合には、当該ログイン証明書が無効であると判定することを特徴とするアクセス権利判定装置。

【請求項 14】請求項 12 および 13 のいずれか一項記載のアクセス権利判定装置において、

前記ログイン証明書には、当該ログイン証明書の発行日時が記録されていて、

前記有効性確認手段は、現在の日時が、前記許可証の発行日時から所定の期間以上経過している場合には、当該ログイン証明書が無効であると判定するものであることを特徴とするアクセス権利判定装置。

【請求項 15】請求項 12、13 および 14 記載のアクセス権利判定装置において、

前記ログイン証明書には、当該ログイン証明書を、最も最近に受信した日時が記録されていて、

前記有効性確認手段は、現在の日時が、前記受信日時から所定の期間以上経過している場合には、当該ログイン証明書が無効であると判定するものであることを特徴とするアクセス権利判定装置。

【請求項 16】請求項 12 から 15 のいずれか一項記載のアクセス権利判定装置において、

前記ログイン証明書には、当該ログイン証明書を受信し

た回数が記録されていて、

前記有効性確認手段は、前記受信回数が、所定の回数を超過している場合には、当該ログイン証明書が無効であると判定するものであることを特徴とするアクセス権利判定装置。

【請求項17】請求項12から16のいずれか一項記載のアクセス権利判定装置において、

前記ログイン証明書には、当該証明書を送信可能な回数が記録されていて、

前記有効性確認手段は、前記送信可能な回数が、所定の回数よりも少ない場合には、当該ログイン証明書が無効であると判定するものであることを特徴とするアクセス権利判定装置。

【請求項18】請求項12から17のいずれか一項記載のアクセス権利判定装置において、

前記依頼者認証手段は、前記有効性確認手段によって、前記証明書が無効であると判断された場合に、他の認証手法によって前記依頼者を特定するものであって、前記証明書発行手段は、前記他の認証手法によって依頼者が特定された場合に、証明書を発行するものであることを特徴とするアクセス権利判定装置。

【請求項19】共有ファイルに対するアクセス権利を持つか否かをコンピュータを用いて判定するためのアクセス権利判定プログラムを格納した記憶媒体において、共有ファイルを要求しているユーザーが、ログインしているクライアント情報処理装置から、当該ユーザーのログイン情報を取得し、上記ユーザーが要求している共有ファイルを、サーバー情報処理装置から取得し、上記取得した共有ファイルに付加されている開示先リストに示されている条件を、上記取得したログイン情報が満足するか否かを判定し、

上記条件が満足されるとき、上記ユーザーは、上記要求した共有ファイルにアクセスする権利があると判定することを特徴とするアクセス権利判定プログラム。

【請求項20】請求項19記載のアクセス権利判定プログラムを格納した記憶媒体において、

上記コンピュータは、上記クライアント情報処理装置にログオンし得る各ユーザーのについての予め定められた属性情報が記述されたユーザー情報ファイルが予め格納されており、

上記ログイン情報は、上記クライアント情報処理装置における上記ユーザーに関するCookieデータであり、

上記開示先リストは、個人に関する予め定められた属性情報が記述され、

上記アクセス権利判定プログラムは、上記Cookieデータが示すユーザーに関する属性を、上記ユーザーファイルから検出し、

上記検出した属性が、上記開示先リストが示す条件を満

足するか否かを判定することを特徴とするアクセス権利判定プログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、共有ファイルを通信回線を介して送受信するための、共有ファイル送受信システムに係り、特に、アクセス制御機能を備える共有ファイル送受信システムに関する。

【0002】

【従来の技術】インターネットと呼ばれる世界的規模のネットワークの普及と共に、このインターネットと企業内ネットワークを接続し、インターネットを介して情報を送受信するケースが増大している。また、前記インターネットにおいては、情報発信機能を持つWWW（World-Wide Web）サーバを利用し、ハイパーテキストと呼ばれる形式の文書ファイルで情報を提供することが一般的となっている。前記ハイパーテキストを解釈し、グラフィカルに表示するソフトウェアはブラウザと呼ばれ、広く普及している。前記ハイパーテキストの言語仕様としては、HTML（HyperText Markup Language）が一般に用いられている。この言語仕様について、および、HTMLで記述されたファイルを表示するためのブラウザについては、例えば、「UNIX MAGAZINE」（ASCII社、1994.10）pp. 52-60に記載されている。なお、殆どのHTMLファイルは、他のHTMLファイルやイメージデータファイルとリンクしており、前記ブラウザは、HTMLファイルを受信した後で、それがリンクしているイメージデータファイルを受信し、該HTMLファイルの内容と合わせて同一画面に表示する。これらHTMLファイルとそれにリンクされたイメージデータファイルを総括してページと呼ぶ。

【0003】上記WWWサーバの多くは、機密情報を含むページを格納するためのアクセス制御機能として、特定の端末に対するページの送信を許可、または拒否する機能や、ユーザーが正しいパスワードを入力することによってページの送信を許可する機能を備えている。これらの機能については、「OPEN DESIGN」（CQ出版社、1997.10）pp. 114-125などに記載されている。

【0004】

【発明が解決しようとする課題】しかし、上述のWWWサーバが持っているアクセス制御機能を利用する場合、WWWサーバに対してアクセス権利の設定を行うことができる者は、WWWサーバの特権ユーザーに限られるという問題がある。

【0005】また、アクセス制御に関する情報が各々のWWWサーバに分散してしまうため、アクセス制御に関する情報を変更する際の手間が大きいという問題がある。

【0006】そして、アクセス制御の設定方法は、WWWサーバ毎に定められているため、個々のWWWサーバ毎にアクセス制御の設定方法を覚えなければならないという問題がある。

【0007】さらに、複数のWWWサーバに跨って情報が保存されている場合には利用者が情報を閲覧するために個々のWWWサーバにログインしなければならないという問題がある。

【0008】本発明の第1の目的は、情報作成者がアクセス権を容易に設定できるようなアクセス制御機能を備えた共有ファイル送受信システムを提供することにある。

【0009】本発明の第2の目的は、アクセス制御に関する情報の変更が容易に行えるアクセス制御機能を備える共有ファイル送受信システムを提供することにある。

【0010】本発明の第3の目的は、情報が複数のWWWサーバに跨っている場合でも、システム全体として一度ログインするだけで、アクセスする権利を持っている、すべてのページにアクセス可能なアクセス制御機能を備える共有ファイル送受信システムを提供することにある。

【0011】本発明の第4の目的は、さまざまなWWWサーバが利用されている環境においても、システム全体としては同一の方法で設定可能なアクセス制御機能を備える共有ファイル送受信システムを提供することにある。

【0012】

【課題を解決するための手段】上記目的を達成するため、本発明の第1の態様によれば、通信回線を介して接続される端末間で共有ファイルを送受するための共有ファイル送受信システムであって、共有ファイルにアクセスする権利をデータ受信側の利用者が有するか否かを判定するためのアクセス権利判定手段と、データ送信側の端末からデータ受信側の端末にファイルを転送するためのデータ中継手段とを備え、前記共有ファイルは、アクセス権利を持つ利用者を示す開示先情報が予め付加され、前記アクセス権利判定手段は、共有ファイルにアクセスする権利をデータ受信側の利用者が持つか否かを、当該共有ファイルに付加されている前記開示先情報に基づいて判定し、前記データ中継手段は、前記データ受信側の利用者の要求に応じてデータ送信側の端末から共有ファイルを受信し、当該受信した共有ファイルに対するアクセス権利を前記利用者が有すると前記アクセス権利判定手段が判定した場合にのみ、前記受信した共有ファイルをデータ受信側の端末に送信することを特徴とする共有ファイル送受信システムが提供される。

【0013】本発明の第2の態様によれば、通信回線を介して接続される端末間で共有ファイルを送受するための共有ファイル送受信システムであって、アクセスする権利を判定するためのアクセス権利判定装置と、データ

受信側の前記端末に前記データを送信するデータ中継装置とが通信回線を介して接続され、前記アクセス権利判定装置は、前記共有ファイルに付加された、アクセスする権利を持つ利用者の条件を、個人に関する予め定められた属性情報が組み合わされて記述されたリストを基に、データ受信側の前記端末の利用者が前記共有ファイルにアクセスする権利を持つか否かを判定し、前記データ中継装置は、データ送信側の端末から前記共有ファイルを受信し、当該共有ファイルに付加されている前記リストを前記アクセス権利判定装置に送信し、前記利用者に当該共有ファイルに対するアクセス権利があると前記アクセス権利判定装置が判定した場合にのみ、データ受信側の前記端末に前記データを送信することを特徴とする共有ファイル送受信システムが提供される。

【0014】本発明の第3の態様によれば、共有ファイルを格納するための機能、および、転送要求を受けた共有ファイルを転送するための機能を有するサーバ装置と、前記サーバ装置から共有ファイルを受信するための機能、および、ユーザーに共有ファイルの情報を表示するための機能を有するクライアント装置と、共有ファイルの転送要求を前記クライアント装置から前記サーバ装置に中継し、共有ファイルを前記サーバ装置から前記クライアント装置に中継するための機能、および、当該共有ファイルをキャッシュするためのキャッシュ機能を有する代理サーバ装置と、前記共有ファイルに付加された、アクセスする権利を持つ利用者の条件を、個人に関する予め定められた属性情報が組み合わされて記述されたリストを基に、前記クライアント装置の利用者が前記共有ファイルにアクセスする権利を持つか否かを判定するためのアクセス権利判定装置と、前記サーバ装置から前記共有ファイルを受信し、当該共有ファイルに付加されている前記リストを前記アクセス権利判定装置に送信し、前記アクセス権利判定装置が前記利用者に当該共有ファイルに対するアクセス権利があると判定した場合にのみ、前記代理サーバ装置に前記データを送信するデータ中継装置とが通信回線を介して接続されていることを特徴とする共有ファイル送受信システムが提供される。

【0015】本発明の第4の態様によれば、通信回線を介して受信した情報を基に、共有ファイルに対するアクセス権利を持つか否かを判断するアクセス権利判定装置であって、通信回線を介して受信する前記情報は、アクセスを許可する利用者の条件を、個人の属性情報を組み合わせて条件式として記述したリストであって、アクセス権利を持つか否かの判断を依頼した依頼者を特定するための依頼者認証手段と、当該アクセス権利判定装置が管理する前記依頼者の属性情報が前記リストを満足する場合には、アクセスする権利を持つと判断するためのアクセス権利判定手段とを備えることを特徴とするアクセス権利判定装置が提供される。

【0016】本発明の第5の態様によれば、通信回線を介して受信した情報を基に、共有ファイルに対するアクセス権利を持つか否かを判断するアクセス権利判定装置であって、通信回線を介して受信する情報とは、前記依頼者の属性情報を、暗号鍵と呼ばれる情報によって暗号化したものと、アクセスを許可する利用者の条件を、個人の属性情報を組み合わせて条件式として記述したリストとであって、当該アクセス権利判定装置は、前記暗号化された属性情報を、前記依頼者が当該アクセス権利判定装置に登録した、復号鍵と呼ばれる情報によって復号する属性情報復号手段を備え、前記アクセス権利判定手段は、前記属性情報復号手段によって復号化した、前記依頼者の属性情報が前記リストを満足する場合には、アクセスする権利を持つと判断するものであることを特徴とするアクセス権利判定装置が提供される。

【0017】本発明の第6の態様によれば、共有ファイルに対するアクセス権利を持つか否かをコンピュータを用いて判定するためのアクセス権利判定プログラムを格納した記憶媒体において、共有ファイルを要求しているユーザーが、ログインしているクライアント情報処理装置から、当該ユーザーのログイン情報を取得し、上記ユーザーが要求している共有ファイルを、サーバ情報処理装置から取得し、上記取得した共有ファイルに付加されている開示先リストに示されている条件を、上記取得したログイン情報が満足するか否かを判定し、上記条件が満足されるとき、上記ユーザーは、上記要求した共有ファイルにアクセスする権利があると判定することを特徴とするアクセス権利判定プログラムを格納した記憶媒体が提供される。

【0018】

【発明の実施の形態】以下、図面を参照して、本発明の実施形態について説明する。

【0019】まず、図1を参照して、本発明がWWW(World-Wide Web)システムに適用されたファイル共有システムの構成の概略について説明する。

【0020】図1において、本実施の形態におけるファイル共有システム10は、WWWのサーバ機能を備えるサーバ情報処理装置11と、WWWのクライアント機能を備えるクライアント情報処理装置12と、前記サーバ情報処理装置11およびクライアント情報処理装置12で送受されるデータを中継する機能を備えるデータ中継処理装置13と、前記中継しようとするデータのアクセス権利を判定するためのアクセス権利判定処理装置14とが、ネットワーク1に接続されて構成されている。

【0021】上記ネットワーク1としては、例えば、企業内のネットワークなどのローカルエリアネットワーク(LAN)が適用され、前記各処理装置が、LANケーブル15を介して相互に接続されて構成される。

【0022】前記アクセス権利判定処理装置14は、前

記サーバ情報処理装置11から前記クライアント情報処理装置12に送信されるデータに対して、前記クライアント情報処理装置12にログインしている利用者(ログインユーザー)(以下、単に、利用者、ユーザーとも称する)が当該データにアクセスする権利を持つかどうかを判定する機能を備える。

【0023】ここで、図1では、ネットワーク1に一つのクライアント情報処理装置12が接続されている場合を示しているが、接続されるクライアント情報処理装置12の数はこれに限らず、クライアント情報処理装置12がLANケーブル15に複数接続されてもよいことは勿論である。

【0024】また、図1では、ネットワーク1に一つのサーバ情報処理装置11が接続されている場合を示しているが、接続されるサーバ情報処理装置11の数はこれに限らず、サーバ情報処理装置11がLANケーブル15に複数接続されてもよいことは勿論である。

【0025】同様に、複数のデータ中継処理装置13がLANケーブル15に接続されていてもよい。また、複数のアクセス権利判定処理装置14がLANケーブル15に接続されていてもよい。

【0026】なお、前記各処理装置は、LANケーブル15に代えて、電話回線などを介して前記ネットワーク1に接続されてもよい。例えば、前記クライアント情報処理装置12と前記データ中継処理装置13とが互いに離れた場所に存在する場合、LANケーブル15に代えて、電話回線などで両者を接続することができる。また、各処理装置相互のデータ転送トラフィックに応じて、より転送容量、速度が大きな伝送路で、特定の処理装置同士を接続することができる。

【0027】前記サーバ情報処理装置11は、中央処理装置(CPU)111と、メモリ112と、LANコントローラ113と、ディスクコントローラ114と、磁気ディスク115とを備えて構成される。

【0028】サーバ情報処理装置は、起動時に、磁気ディスク115に格納されているオペレーティングシステム(OS)115aおよびWWWサーバプログラム115bを、ディスクコントローラ114を介して、メモリ112上にロードする。そして、CPU111がWWWサーバプログラム115bを実行することで、WWWサーバとして機能する。

【0029】すなわち、サーバ情報処理装置11は、磁気ディスク115にHTML(HyperText Markup Language)ファイルや画像ファイルを格納したり、クライアント情報処理装置12がデータ中継処理装置13を介して要求した、HTMLファイル、または、これに加えて、当該HTMLファイル200にリンク(参照指定)された画像ファイル、動画ファイル、音声ファイルなど(以下、被参照ファイルともいう)を、前記クライアント情報処理装置12に転送す

る。

【0030】WWWサーバプログラム115bとしては、WWWシステムに用いられる既存のプログラムを変更することなく、そのまま使用することができる。

【0031】なお、WWWサーバプログラム115bは、当該WWWサーバプログラム115bが備えるアクセス制御機能を利用して、データ中継処理装置13からのアクセスのみを受け付けるように設定されている。

【0032】前記クライアント情報処理装置12は、CPU121と、メモリ122と、LANコントローラ123と、ディスクコントローラ124と、磁気ディスク125とを備えて構成される。

【0033】クライアント情報処理装置12は、起動時に、磁気ディスク125に格納されているOS125aを、ディスクコントローラ124を介して、メモリ122にロードする。

【0034】また、クライアント情報処理装置12は、ユーザーの指示に従い、ブラウザプログラム125bを、ディスクコントローラ124を介して、磁気ディスク125からメモリ122上にロードする。そして、CPU121がブラウザプログラム125bを実行することで、WWWクライアントの機能を実現している。すなわち、クライアント情報処理装置12は、WWWクライアントとして、ユーザーが要求するHTMLファイルや被参照ファイルなどの転送を前記サーバ情報処理装置11に要求し、また、前記サーバ情報処理装置11から転送されてきたHTMLファイル、または、これに加えて画像ファイルなどの被参照ファイルを表示する。

【0035】なお、ブラウザプログラム125bは、プロキシサーバ（代理サーバ）を設定する機能を利用して、前記サーバ情報処理装置11とデータの送受を行う際には、必ず前記データ中継装置13を介して行うように設定されている。

【0036】ブラウザプログラム125bとしては、プロキシサーバを利用できるものであれば、WWWシステムに用いられる既存のプログラムを変更することなく、そのまま使用することができる。

【0037】また、クライアント情報処理装置12は、ユーザーの指示に従い、アクセス権利設定プログラム125cを、ディスクコントローラ124を介して、磁気ディスク125からメモリ122にロードする。

【0038】アクセス権利設定プログラム125cは、HTMLファイルに対して、アクセス権利を設定するためのものである。HTMLファイルとしては、ユーザーが作成するなどして、予め磁気ディスク125に格納されているものを想定して説明するが、アクセス権利の設定を行いつつ、作成するものであってもよい。

【0039】前記データ中継処理装置13は、CPU131と、メモリ132と、LANコントローラ133と、ディスクコントローラ134と、磁気ディスク13

5とを備えて構成される。

【0040】データ中継処理装置13は、起動時に磁気ディスク135に格納されているOS135aと、データ中継処理プログラム135bとをディスクコントローラ134を介して、メモリ132にロードする。データ中継処理プログラム135bは、前記クライアント情報処理装置12から送信されてきた、HTMLファイルや被参照ファイルなどの転送要求を前記サーバ情報処理装置11に送信したり、前記サーバ情報処理装置11から送信されてきたHTMLファイルや画像ファイルに対して、ユーザーがアクセスする権利を持つかどうかを前記アクセス権利判定装置14に確認し、アクセスする権利を持つ場合には当該HTMLファイルや画像ファイルを前記クライアント情報処理装置12に送信するためのものである。

【0041】前記アクセス権利判定装置14は、CPU141と、メモリ142と、LANコントローラ143と、ディスクコントローラ144と、磁気ディスク145とを備えて構成される。

【0042】アクセス権利判定装置14は、起動時に、磁気ディスク145に格納されているOS145aと、アクセス権利判定プログラム145bとをディスクコントローラ144を介して、メモリ142にロードする。

【0043】なお、アクセス権利判定装置14は、パスワード管理ファイル145cと、ユーザーID情報ファイル145dと、共有グループ定義ファイル145eとを磁気ディスク145に格納している。

【0044】アクセス権利判定プログラム145bは、ユーザーのパスワード情報をパスワード管理ファイル145cによって管理する。前記パスワード情報は、前記アクセス権利判定プログラム145bの指示によって前記メモリ142にロードされ、ユーザーを特定するために用いられる。

【0045】また、アクセス権利判定プログラム145bは、ユーザーID情報ファイル145dによって予め定義されているユーザーの個人情報、および、共有グループ定義ファイル145eによって予め定義されている共有グループ情報を管理する。前記ユーザーID情報および前記共有グループ定義情報は、前記アクセス権利判定プログラム145bの指示によって前記メモリ142にロードされ、アクセスする権利を持つか否かを判定するために用いられる。

【0046】以下、上述したファイル共有システム10の主な構成について、詳細に説明する。

【0047】まず、図2を参照して、前記ユーザーID情報ファイル145dについて説明する。

【0048】ユーザーID情報ファイル145dでは、個人に関する属性のカテゴリを示す情報と、属性の内容を示す情報とが互いに対応付けられ、情報の組として記述される。ユーザーID情報ファイル145dによって



記述される属性のカテゴリの数は、1つであっても、複数であってもよい。複数のカテゴリについて、属性を記述する場合、1つのカテゴリについて属性を記述する情報の組を、複数組記述することが好適である。

【0049】図2に示されるユーザーID情報ファイル145dは、10組の情報の組が記述され、10のカテゴリについて、属性を登録している。そして、カテゴリを示す情報として、カテゴリを識別するためのカテゴリ番号が用いられている。また、いくつかのカテゴリについて、そのカテゴリの属性の内容を示す情報として、予め定められたコードが用いられている。

【0050】なお、本実施の形態では、ユーザーID情報ファイル145dに登録され得るカテゴリは予め定められ、これらのカテゴリを予め定められた順序で、欠番および重複なくなく並べる形式としている。すなわち、属性の内容を示す情報が、予め定められた順番で並べられ、その情報が現れる順番によりカテゴリを示している。このため、アクセス権利判定装置14（図1参照）の前記磁気ディスク145（図1参照）に実際に記憶されるのは、属性の内容を示すデータだけ、あるいは、データに加えてコードの値とすることができる。

【0051】次に、図3を参照して、前記共有グループ情報ファイル145e（図2参照）について説明する。

【0052】図3において、共有グループ情報ファイル145eは、共有グループ情報と、当該共有グループ情報の名称と、当該共有グループの作成者の識別子と、作成日時とが互いに対応付けられた情報組が、1組または複数組登録される。図3に示される例では、6組の情報組が登録されている。

【0053】前記共有グループ情報145eにおいては、アクセスを許可する条件がリスト形式で記述されている。以下、このリストを開示先リストと呼ぶ。

【0054】開示先リストは、アクセスを許可すべきユーザーの条件（以下、追加条件という）、または、アクセスを拒否すべきユーザーの条件（以下、除外条件という）が記述される項を少なくとも1つ含む。項は、その項が追加条件を示すか、除外条件を示すかを示す区切り記号に続けて記述され、複数の項が含まれる場合、区切り記号により区切られて並べられる。前記追加条件を示す区切り記号としては、カンマ（,）が用いられ、前記除外条件を示す区切り記号としては、マイナス（-）が用いられる。ただし、追加条件を示す項が、開示先リストの先頭に現れる場合には、その項の区切り記号（,）は省略される。

【0055】前記項は、ユーザーの条件が関係演算子で記述された条件式を少なくとも1つ含む。条件式は、ユーザーの条件を、ユーザーID情報ファイル145dにおける属性、または、他のグループを示すグループ名称を指定するためのものである。共通する項に、複数の条件式が含まれる場合、条件式と条件式とは、論理演算子

（^）で連結される。この論理演算子（^）は、論理積の意味を持つ。

【0056】各条件式は、「カテゴリ番号」と、「グループ/データ/コード識別子」と、「関係演算子」と、「条件データ」とが互いに対応付けられて記述されている。

【0057】前記「カテゴリ番号」は、条件の指定に用いるデータのカテゴリを示すためのものである。

【0058】前記「グループ/データ/コード識別子」は、前記カテゴリ番号により示されるカテゴリにおけるデータの種類の識別するためのものである。グループ/データ/コード識別子としては、条件の指定に用いられるデータの種類の、他の開示先リストにより定義されたグループ名称で記述されることを示すG（Group）と、ユーザーID情報ファイル145dにおけるデータの情報を示すD（Data）と、ユーザーID情報ファイル145dにおけるコードの情報を示すC（Code）とを用いることができる。

【0059】前記「条件データ」は、関係演算子と共に、条件を指定するためのものであり、前記「カテゴリ番号」および「グループ/データ/コード識別子」で指定された情報に対応して、「条件データ」としては、グループ名称、データ、コードのいずれかが用いられる。前記関係演算子、としては、等しい（=）、等しくない（≠）、大きい（>）、小さい（<）を用いることができる。なお、前記「条件データ」が数値以外の文字列である場合、文字コードの数値を用いて、関係演算子が指定する関係を定義することができることで、前記関係演算子の演算は、前記論理演算子および区切り記号の演算に先行して演算され、また、前記論理演算子の演算は、区切り記号の演算に先行して演算される。なお、区切り記号の演算は、左から右に順番に演算される。

【0060】例えば、図2で示した前記ユーザーID情報145dの定義と、図3で示した前記共有グループ情報145eとを用いた場合、「本社の資材グループと、システム研究所の第四部の主任以上と、暗号太郎」という開示先に対する共有グループ情報は、「OG=本社資材、5C=676^6C=04^8C>=5、2D=暗号太郎」という開示先リストになる。すなわち、この開示先リストは、追加条件を示す項3つで記述され、このうち、第2項は、3つの条件式の論理積で記述されている。

【0061】また、「本社のうちの営業以外と、システム研究所のうちの安全課以外とであって、かつ、氏名コード6781901001および678951010を除く」という開示先に対する共有グループ情報は、「5C=001^6C≠21、5C=676^7C≠402-4C=6781901001-4C=678951010」という開示先リストになる。すなわち、この開示先リストは、追加条件を示す項2つと、除外条件を示す項2つとで記述され、このうち、第1項

および第2項は、それぞれ2つの条件式の論理式で記述されている。

【0062】次に、図4を参照して、アクセス権利をHTMLファイルに対して設定する方法、および、アクセス権利が設定されたHTMLファイルについて説明する。

【0063】図4(a)において、HTMLファイル300は、サーバー情報処理装置11(図1参照)のユーザー(以下、HTMLファイルのオーナー、または、単にオーナーともいう)が作成したHTMLファイルの例である。ユーザーは、テキストエディタやHTMLエディタなどを用いて、図4(a)に示すようなHTMLファイルを作成することができる。

【0064】ここで、HTMLファイルのオーナーとは、当該HTMLファイルにアクセスする権利を設定する権利を持つ者を指し、当該HTMLファイルを作成した者だけでなく、このファイルを改変する権利を持つ者、および、アクセス権利を設定、変更する権利のみを有する者を含み、一人のユーザーである場合だけでなく、複数人のユーザーが属するグループなどであってもよい。

【0065】なお、上記アクセス権利を設定、変更する権利のみを有する者とは、例えば、サーバー情報処理装置11(図1参照)において、HTMLファイルを書き換える権利はないが、アクセス権利設定プログラム125cを実行する権利は有する者として設定することができる。

【0066】次に、HTMLファイルのオーナーは、前記アクセス権利設定プログラム125cによって、HTMLファイルにアクセス権利を設定する。

【0067】図4(b)において、HTMLファイル400は、図4(a)に示されるHTMLファイル300に、アクセス権利が設定されたHTMLファイルの例である。

【0068】アクセス権利が設定されたHTMLファイル400は、アクセス権利が設定される前のHTMLファイル420の先頭部分に、アクセス制御のためのヘッダ410(以降、当該ヘッダをアクセス制御ヘッダと呼ぶ)410を付加したものになっている。

【0069】図4(c)を参照して、HTMLファイル400(図4(b)参照)における、アクセス制御ヘッダ410(図4(b)参照)の詳細について説明する。

【0070】図4(c)において、前記アクセス制御ヘッダ410は、アクセス制御ヘッダであることを示す文字列を記述するための領域411と、当該HTMLファイルにアクセス権利を設定したオーナーの識別子を記述するための領域412と、当該HTMLファイルにアクセス権利を設定した日付を記述するための領域413と、当該HTMLファイルにアクセスを許可するユーザー条件の開示先リストを記述するための領域414と、

当該HTMLファイルにアクセスする権利がない場合に表示すべきメッセージが格納されたメッセージファイルを示すリンク情報(参照先を指定する情報)を記述するための領域415と、当該HTMLファイルのアクセス権利を判定するアクセス権利判定装置14(図1参照)のホスト名を記述するための領域416とを含んで構成される。

【0071】前記領域415に記録されている、アクセスする権利がない場合に表示するメッセージファイルのリンク情報は、例えば、WWWシステムに適用される場合、URL(Uniform Resource Locators)形式で記述することが便利である。アクセスする権利がない場合に表示すべきメッセージを記録したファイルは、前記サーバー情報処理装置11(図1参照)の磁気ディスク115(図1参照)に格納されている。なお、メッセージファイルのリンク情報に代えて、メッセージそのものを格納してもよい。また、当該HTMLファイルにアクセスする権利がない場合であっても、メッセージを表示せず、ユーザー透過的な情報提示態様とすることも可能である。この場合、メッセージ、または、それを格納したメッセージファイルを、前記領域415に格納することは省略される。

【0072】ここで、前記アクセス制御ヘッダ部分410は、HTMLにおけるコメントを記述する文法を利用して記述されている。このため、当該HTMLファイルをブラウザプログラムで直接表示した場合でも、余分な情報が表示されることや、画面が乱れること、を防ぐことができる。

【0073】アクセス権利が設定されたHTMLファイル400は、通常のHTMLファイルと同様に、前記サーバー情報処理装置11(図1参照)の磁気ディスク115(図1参照)に格納される。

【0074】次に、図5、6、および、図9から12を参照して、アクセス権利設定プログラム125cについて説明する。

【0075】まず、図6を参照して、アクセス権利設定プログラム125cのモジュール構成について説明する。

【0076】図6において、アクセス権利設定プログラム125cは、ログイン処理ルーチン1100と、アクセス権利設定ルーチン1200と、ログアウト処理ルーチン1300とを含んで構成される。

【0077】次に、図5を参照して、アクセス権利設定プログラム125cの動作フローについて説明する。

【0078】図5において、アクセス権利設定プログラム125cは、まず、ステップ1001で、前記ログイン処理ルーチン1100を実行し、アクセス権利を設定しようとしているユーザーを特定するための処理を行う。ログイン処理ルーチン1100は、アクセス権利を設定しようとしているユーザーを特定するため(すなわ

10

20

30

40

50

ち、当該HTMLファイルのオーナーであるか否かを判定するため)に、アクセス権利判定プログラム145bに対してログイン処理を行うためのものである。ログイン処理ルーチン1100におけるログイン処理では、前記アクセス権利判定プログラム145bに何度もログインすることを防止するため、ログイン証明書を用いる。ログイン証明書は、アクセスしているユーザーが、過去に前記アクセス権利判定プログラム145bにログインした正当なユーザーであることを保証するものである。ログイン処理ルーチン1100における処理の詳細については後述する。

【0079】次に、ユーザーの特定が成功したか否かを判定する(ステップ1002)。ユーザーの特定に成功したと判定された場合には、ステップ1003に移行し、イベント待ち状態をとる。イベントが到着すると、イベントがアクセス権利設定要求か否かを調べる(ステップ1004)。

【0080】アクセス権利設定要求である場合には、ステップ1008に移行し、前記アクセス権利設定ルーチン1200を実行して、ステップ1003に戻る。一方、アクセス権利設定要求でない場合には、ステップ1005に移行し、イベントがログアウト要求か否かを調べる。

【0081】ログアウト要求であれば、前記ログアウト処理ルーチン1300を実行し、ログアウト処理を行う。ステップ1007で、ログアウトに成功すると、プログラムを終了する。一方、ログアウトに失敗した場合には、ステップ1003に戻る。

【0082】図9を参照して、ログイン証明書の構成について説明する。

【0083】図9において、ログイン証明書200は、ログイン証明書の識別番号を記述するための領域201と、前記ユーザーの識別子を記述するための領域202と、ログイン証明書の発行日時を記録するための領域203と、当該ログイン証明書を使用してアクセスを行った回数を記述するための領域204と、当該ログイン証明書を使用して最後にアクセスを行った日時を記録するための領域205とを含んで構成されている。

【0084】なお、本実施の形態におけるログイン証明書の形式は、Cookieと呼ばれる形式を利用している。Cookieは、ブラウザの状態を保存するために一般的に用いられている形式である。前記ブラウザプログラム125bがログイン証明書を保持することが、Cookieの形式を利用することにより可能となる。従って、後述するHTMLファイルを閲覧する際に、前記ブラウザプログラム125bが、前記クライアント情報処理装置12の利用者を特定することができる。

【0085】図10を参照して、アクセス権利設定プログラムにおける前記ログインルーチン1100の動作フローについて説明する。

【0086】まず、ログイン証明書を持っているかどうかを調べる(ステップ1101)。ログイン証明書を持っている場合には、ログイン証明書が有効であるかどうかを調べるためにログイン証明書を前記アクセス権利判定プログラム145bに送信する(ステップ1102)。

【0087】次に、送信したログイン証明書が有効かどうかの判定結果を受信する(ステップ1103)。ログイン証明書が有効であった場合には、ステップ1007以下を実行して、新しいログイン証明書の発行と、古いログイン証明書の破棄を行い、処理を終了する。

【0088】一方、ログイン証明書が有効でなかった場合には、IDとパスワードとをユーザーから取得する(ステップ1104)。次に、ユーザー認証処理を行う(ステップ1105)。ユーザー認証処理においてログインに成功した場合には、新しいログイン証明書の発行(ステップ1107)と、古いログイン証明書の破棄(ステップ1108)とを行い、処理を終了する。

【0089】ステップ1105におけるユーザー認証処理でログインに失敗した場合には、ステップ1109に移行し、3回続けて失敗するまでは、ステップ1104～ステップ1106の処理を繰り返すように制御する。3回続けて失敗した場合には、ステップ1108を実行する。

【0090】なお、本実施の形態では、ログイン証明書が有効かどうかを確認するための処理をアクセス権利判定プログラム145bで行っているが、この処理を、ログイン処理ルーチンに処理1100を組み込んでよい。

【0091】図11を参照して、アクセス権利設定プログラム125cの前記ログアウト処理ルーチン1300の動作フローについて説明する。ログアウト処理ルーチン1300は、アクセス権利判定プログラム145b(図6参照)に対してログアウト処理を行うためのものである。

【0092】図11において、まず、ステップ1301で、現在オープン中のファイルがあるかどうかを調べる。オープン中のファイルがない場合には、ステップ1304以下を実行し、アクセス権利判定プログラム145bからのログアウト処理を行う。オープン中のファイルがある場合には、ログアウト処理を中断するかどうかをユーザーに確認する(ステップ1302)。ログアウト処理を中断する場合には、処理を終了する。ログアウト処理を続行する場合には、ステップ1303で、オープン中のファイルをクローズする。次に、ステップ1304で、前記アクセス権利判定プログラム145bにログイン証明書を送信し、ログイン証明書を無効化する。

【0093】図12を参照して、アクセス権利設定プログラムの前記アクセス権利設定ルーチン1200の動作フローについて説明する。アクセス権利設定ルーチン1

200は、ユーザーが作成したHTMLファイルにアクセス権利を設定するためのものである。すなわち、サーバ情報処理装置11（図1参照）のユーザーが、当該ユーザーがオーナーであるHTMLファイルのアクセス権利を設定するために用いられる。

【0094】まず、ステップ1201で結果を一時的に出力する一時ファイルを作成する。次に、ステップ1202で前記開示先リストを作成する。ステップ1203では、作成した開示先リストを含めたヘッダ部分を一時ファイルに書き込む。次に、ステップ1204でアクセス権利を設定するHTMLファイル（以降、入力ファイルと呼ぶ）のデータをバッファに読み込む。次に、ステップ1205で入力ファイルから、すべてのデータを読み込み終えたかどうかを調べる。これは、読み込んだデータのサイズが0であれば、入力ファイルから、すべてのデータを読み込み終えたと判断する。入力ファイルから、すべてのデータを読み込み終えていない場合には、ステップ1206で一時ファイルに読み込んだデータを書き込み、ステップ1204に戻る。一方、入力ファイルのすべてのデータを読み込み終えている場合には、入力ファイルをクローズし（ステップ1207）、一時ファイルもクローズする（ステップ1208）。次に、ステップ1209で、アクセス権利を設定したHTMLファイル（以降、出力ファイルと呼ぶ）のファイル名が入力ファイルのファイル名と一致しているかどうかを調べる。ファイル名が一致していない場合には、一時ファイルのファイル名を出力名に変更し、処理を終了する。一方、ファイル名が一致している場合には、ステップ1210で入力ファイルを削除した後、一時ファイルのファイル名を出力ファイル名に変更し、処理を終了する。

【0095】図13を参照して、ユーザーが、アクセス権利が設定されたHTMLファイルを閲覧する場合の動作の概略について説明する。図13には、アクセス権利が設定されたHTMLファイルを、前記サーバ情報処理装置11と前記クライアント情報処理装置12との間で送受する場合に、本実施の形態における各プログラム間で送受されるデータのフローが描かれている。

【0096】図13において、まず、ユーザーは、前記ブラウザプログラム125bにHTMLファイルを要求する。

【0097】次に、前記ブラウザプログラム125bは、前記データ中継プログラム135bに前記要求を転送する。転送に際し、前記ブラウザプログラム125bが前記ログイン証明書を保持している場合には、当該ログイン証明書も同時に転送する。前記データ中継プログラム135bは、前記WWWサーバプログラム115bに前記要求を転送し、前記WWWサーバプログラム115bから要求したHTMLファイルを受信する。HTMLファイルを受信した、前記データ中継プログラム135bは、前記アクセス権利判定プログラム145bに対

して、ログイン証明書を転送し、ユーザー認証処理を行う。

【0098】次に、前記データ中継プログラム135bは、HTMLファイルから開示先リストを取り出し、前記アクセス権利判定プログラム145bに転送する。前記アクセス権利判定プログラム145bは、開示先リストの条件にユーザーのID情報が適合するかどうかを調べ、結果を前記データ中継プログラム135bに通知する。前記結果を受信した前記データ中継プログラム135bは、前記アクセス権利判定プログラム145bが「ユーザーは当該HTMLファイルに対しアクセス権利を持つ」と判定した場合には、当該HTMLファイルを前記ブラウザプログラム125bに転送する。一方、前記アクセス権利判定プログラム145bが「ユーザーは当該HTMLファイルに対してアクセス権利を持たない」と判定した場合には、当該HTMLファイルからエラーメッセージファイルのファイル名を取り出し、前記WWWサーバプログラム115bにエラーメッセージファイルを要求する。そして、前記WWWサーバプログラム115bから受信したエラーメッセージファイルを前記ブラウザプログラム125bに転送する。最後に、前記ブラウザプログラム125bは、前記データ中継プログラム135bから受信した、ファイルを前記クライアント情報処理装置12の画面に表示する。

【0099】次に、図20から図22を参照して、HTMLファイルの転送を要求した場合に表示される画面について説明する。

【0100】図20は、図4（b）の前記HTMLファイルに対してアクセスする権利を持つユーザーが、図4（b）の前記HTMLファイルの転送を要求した場合に表示される画面の例である。

【0101】一方、図21は、図4（b）の前記HTMLファイルに対してアクセスする権利を持たないユーザーが、図4（b）の前記HTMLファイルの転送を要求した場合に表示される画面の例である。なお、この例では、前記サーバ情報処理装置11には、エラーメッセージファイルとして、図22のファイルが格納されている。

【0102】次に、図8、14、15を参照して、前記データ中継処理プログラム135bについて説明する。

【0103】まず、図8を参照して、前記データ中継処理プログラム135bのモジュール構成について説明する。

【0104】前記データ中継処理プログラム135bは、ログイン処理ルーチン2000と、ログアウト処理ルーチン2100と、データ中継処理ルーチン2200と、アクセス権利確認ルーチン2300とを含んで構成される。

【0105】前記データ中継処理ルーチン2200は、サーバ情報処理装置11とクライアント情報処理装置1

2との間で行われる、データの送受を中継するためのものである。

【0106】次に、図14を参照して、データ中継処理ルーチン2200の動作フローについて説明する。

【0107】まず、ステップ2201で、前記ブラウザプログラム125bからの要求を待ち受ける。要求がくると、ステップ2202で、要求にログイン証明書が含まれているかどうかを調べる。ログイン証明書が含まれていない場合には、ステップ2204以下を実行する。ログイン証明書が含まれている場合には、ログイン証明書を取り出し、ステップ2204以下を実行する。ステップ2204では、ブラウザプログラム125bからの前記要求がログアウト要求であるかどうかを調べる。本実施の形態では、前記データ処理ルーチンは、前記WWWサーバ115bに格納されている、ある特定のHTMLファイルの転送を要求することを、ログアウト要求として解釈する。ログアウト要求である場合には、ログアウト処理を実行し（ステップ2217）、ステップ2201に戻る。ログアウト要求でなかった場合には、前記WWWサーバプログラム115bに前記要求を転送する。次に、前記WWWサーバプログラム115bからHTMLファイルを受信する。ステップ2207で、前記HTMLファイルにアクセス権利が設定されているかどうかを調べ、アクセス権利が設定されていなければ、ステップ2212で、前記HTMLファイルを前記ブラウザプログラム125bに送信する。一方、アクセス権利が設定されている場合には、ステップ2208に移行し、ログイン処理ルーチン2000をコールし、ログイン処理を行う。次に、ステップ2208のログイン処理が成功したかどうかを調べ、ログインに失敗した場合には、エラーメッセージを前記ブラウザプログラム125bに転送し、ステップ2201に戻る。一方、ログインに成功した場合には、ステップ2210で、前記アクセス権利確認ルーチン2300をコールし、ユーザーが前記HTMLファイルに対するアクセス権利を持つかどうかを調べる。アクセス権利を持つ場合には、前記HTMLファイルを前記ブラウザプログラム125bに送信し（ステップ2212）、ステップ2201に戻る。一方、アクセス権利を持たない場合には、前記HTMLファイルからエラーメッセージファイルのURLを取り出し（ステップ2213）、前記WWWサーバプログラム115bにエラーメッセージファイルの転送を要求する（ステップ2214）。次に、ステップ2215で、前記WWWサーバプログラム115bからエラーメッセージファイルを受信し、前記ブラウザプログラム125bに前記エラーメッセージファイルを転送する（ステップ2216）。ファイルの転送が終了するとステップ2201に戻る。

【0108】ログイン処理ルーチン2000、およびログアウト処理ルーチン2100は、前記アクセス権利設

定プログラム125cのログイン処理ルーチン1100、ログアウト処理ルーチン1300と同じ処理を行うため、ここでは説明を省略する。

【0109】次に、図15を参照して、前記アクセス権利確認ルーチン2300の動作フローについて説明する。アクセス権利確認ルーチン2300は、前記WWWサーバプログラム115bから受信したHTMLファイルにユーザーがアクセスする権利を持つかどうかを前記アクセス権利判定プログラム145bに確認するためのものである。

【0110】まず、ステップ2301で、アクセス権利が設定されたHTMLファイルから、開示先リストを取り出す。次に、ステップ2302で、アクセス権利を持つかどうかを判定するため、前記開示先リストを前記アクセス権利判定プログラム145bに送信する。次に、ステップ2303で、アクセス権利判定プログラム145bから判定結果を受信し、処理を終了する。

【0111】次に、図7、16から19を参照して、前記アクセス権利判定プログラム145bについて説明する。

【0112】まず、図7を参照して、前記アクセス権利判定プログラム145bのモジュール構成について説明する。

【0113】図7において、前記アクセス権利判定プログラム145bは、ログイン処理ルーチン3100と、アクセス権利判定ルーチン3200と、ログアウト処理ルーチン3300とを含んで構成される。

【0114】次に、図16を参照して、前記アクセス権利判定プログラム145bの動作フローについて説明する。

【0115】まず、アクセス権利判定プログラム145bは、ステップ3001で、前記データ中継処理プログラム135bや前記アクセス権利設定プログラム125cからのアクセスを待ち受ける。（以降、アクセス権利判定プログラム145bに対してアクセスを行う、前記データ中継処理プログラム135bや前記アクセス権利設定プログラム124cをクライアントと総称する。）アクセス要求を受信すると、ステップ3002で、その要求がログイン要求であるかどうかを調べる。ログイン要求の場合には、ログイン処理を行い、ステップ3001で、クライアントからの要求待ち状態に戻る。ログイン要求でない場合には、ステップ3003で、その要求がアクセス権利判定要求であるかどうかを調べる。アクセス権利判定要求の場合には、アクセス権利判定処理を行い、ステップ3001に戻る。アクセス権利判定要求でない場合には、ステップ3004で、ログアウト要求かどうかを調べる。ログアウト要求の場合には、ログアウト処理を行い、ステップ3001に戻る。ログアウト要求でない場合には、ステップ3001に戻る。

【0116】次に、図17を参照して、前記ログイン処

理ルーチン3100の動作フローについて説明する。ログイン処理ルーチン3100は、アクセスを行うユーザーを特定するためのものである。

【0117】まず、ステップ3101で、クライアントからユーザーIDを取得する。次に、パスワード情報ファイルから、ユーザーのパスワード情報を読み込み、ユーザー認証処理を行う。ステップ3104で、ユーザー認証処理が成功したかどうかを調べ、成功した場合には、新しいログイン証明書を発行する（ステップ3105）。一方、ユーザー認証処理が失敗した場合には、ステップ3106に移行し、3回続けて失敗するまでは、ステップ3101～ステップ3104の処理を繰り返すように制御する。

【0118】次に、図18を参照して、前記アクセス権利判定ルーチン3200の動作フローについて説明する。アクセス権利判定ルーチン3200は、ログインしているユーザーが、前記クライアントから送信されてきた開示先リストの条件に適合するかどうかを判定するためのものである。

【0119】まず、ステップ3201で、クライアントがログイン証明書を持っているかどうかを調べる。ログイン証明書を持っている場合には、ステップ3202で、そのログイン証明書が有効かどうかを調べる。ログイン証明書が有効であった場合には、ステップ3205以下を実行する。一方、ステップ3201でログイン証明書を持っていなかった場合や、ステップ3202でログイン証明書が有効でなかった場合には、ログイン処理を行い、ログイン処理が失敗した場合には、そのまま処理を終了する。ログインに成功すると、ステップ3205に移行し、ログインしたユーザーのユーザーID情報を読み込む。次に、クライアントから開示先リストを受信し（ステップ3206）、開示先リストの条件を、ログインしているユーザーが満足するかどうかを調べる（ステップ3207）。ユーザーが条件を満足する場合には、クライアントに「アクセス権あり」を通知し（ステップ3209）、処理を終了する。一方、ユーザーが条件を満足しない場合には、クライアントに「アクセス権なし」を通知し（ステップ3210）、処理を終了する。

【0120】なお、本実施の形態では、前記アクセス権利判定プログラム145bは既に無効化されたログイン証明書を保持しており、前記ログイン証明書が、既に無効化されたログイン証明書と一致する場合や、前記ログイン証明書の発行日時を記録するための領域503に記述されている値が、現在時刻から1日以上古い値である場合や、前記ログイン証明書のアクセス回数を記録するための領域504に記述されている値が、100を超えている場合や、前記ログイン証明書の最終アクセス時刻を記録するための領域505に記述されている値が、現在時刻から1時間以上古い値である場合には、当該ログ

イン証明書は無効であると判断する。

【0121】また、前記クライアント情報処理装置12（図1参照）から、前記アクセス権利判定装置14（図1参照）に、ユーザーの属性情報を転送するに際し、クライアント情報処理装置12において、当該属性情報を予め定められた情報を暗号鍵として暗号化した状態で送信することができる。この場合、上記暗号鍵に対応する復号鍵を前記アクセス権利判定装置14に予め格納しておき、当該復号鍵を用いて前記暗号化された属性情報を復号化する復号機能を前記アクセス権利判定プログラム145b（図1参照）に設けておく。前記アクセス権利判定装置14において、受信したユーザーの属性情報を前記復号機能により復号化した属性情報が、共有ファイルに付加されている開示先リストが示す条件を満たす否かによって、アクセスする権利の有無を判定することができる。

【0122】次に、図19を参照して、前記ログアウト処理ルーチン3300の動作フローについて説明する。ログアウト処理ルーチン3300は、ログインしているユーザーがアクセスを終了することを宣言するためのものである。

【0123】まず、ステップ3301で、ログイン証明書が有効か否か、すなわち、ログイン証明書が既に無効化されているかどうかを調べる。

【0124】既に無効化されたログイン証明書であった場合には、処理を終了する。

【0125】一方、未だ無効化されていないログイン証明書であった場合には、当該ログイン証明書を無効化されたログイン証明書として保持してログイン証明書を無効化（ステップ3302）し、処理を終了する。

【0126】

【発明の効果】以上説明したように、本発明によれば、HTMLファイルに付加された開示先リストを基にしてアクセス制御を行うため、WWWサーバに対して特別な権利を持たない情報作成者でもアクセス権を容易に設定することができる。。

【0127】また、本発明によれば、アクセス権利判定装置がユーザーの属性情報を一括して管理し、アクセス制御に関する情報の変更は、HTMLファイルに付加された開示先リストを変更するのではなく、アクセス権利判定装置が管理しているユーザーの属性情報を変更することによって行うことができる。従って、アクセス制御に関する情報の変更が容易に行うことができる。

【0128】さらに、本発明によれば、WWWサーバが持っているアクセス制御機能を使用せず、データ中継処理プログラムがアクセス制御を行うことができる。このため、さまざまなWWWサーバが利用されている環境においても、システム全体としては同一の方法でアクセス制御を行うことができる。

【0129】そして、本発明によれば、最初のログイン

時にログイン証明書を発行し、当該ログイン証明書を使用して以降のアクセスにおけるユーザーを特定することができる。このため、情報が複数のWWWサーバに跨っている場合でもシステム全体として一度ログインするだけで、アクセスする権利を持っているページのすべてにアクセスすることが可能となる。

【図面の簡単な説明】

【図1】 本発明の一実施形態が適用されたファイル共有システムの概略構成図である。

【図2】 ユーザーID情報ファイル145dの内容の一例を示す図である。

【図3】 共有グループ情報ファイル145eの内容の一例を示す図である。

【図4】 HTMLファイル、アクセス権利が設定されたHTMLファイル、アクセス制御ヘッダの一例を示す図である。

【図5】 アクセス権利設定プログラム125cの動作フローを示した図である。

【図6】 アクセス権利設定プログラム125cのモジュール構成を表した図である。

【図7】 アクセス権利判定プログラム145bのモジュール構成を表した図である。

【図8】 データ中継処理プログラム135bのモジュール構成を表した図である。

【図9】 ログイン証明書の構成の一例を示す図である。

【図10】 アクセス権利設定プログラム125cのログイン処理ルーチン1000の動作フローを示した図である。

【図11】 アクセス権利設定プログラム125cのログアウト処理ルーチン1100の動作フローを示した図である。

【図12】 アクセス権利設定プログラム125cのアクセス権利設定ルーチン1200の動作フローを示した図である。

【図13】 アクセス権利が設定されたHTMLファイルを、サーバ情報処理装置11とクライアント情報処理装置12との間で送受する場合に、本実施の形態の各プログラム間で送受されるデータのフローの概略を示した図である。

【図14】 データ中継プログラム135bのデータ中継処理ルーチン2200の動作フローを示した図である。

【図15】 データ中継プログラム135bのアクセス権利確認ルーチン2300の動作フローを示した図である。

【図16】 アクセス権利判定プログラム145bの動

作フローを示した図である。

【図17】 アクセス権利判定プログラム145bのログイン処理ルーチン3100の動作フローを示した図である。

【図18】 アクセス権利判定プログラム145bのアクセス権利判定ルーチン3200の動作フローを示した図である。

【図19】 アクセス権利判定プログラム145bのログアウト処理ルーチン3300の動作フローを示した図である。

【図20】 アクセス権利が設定されたHTMLファイルを、アクセスする権利を持つユーザーが閲覧しようとする場合に表示される、画面の一例である。

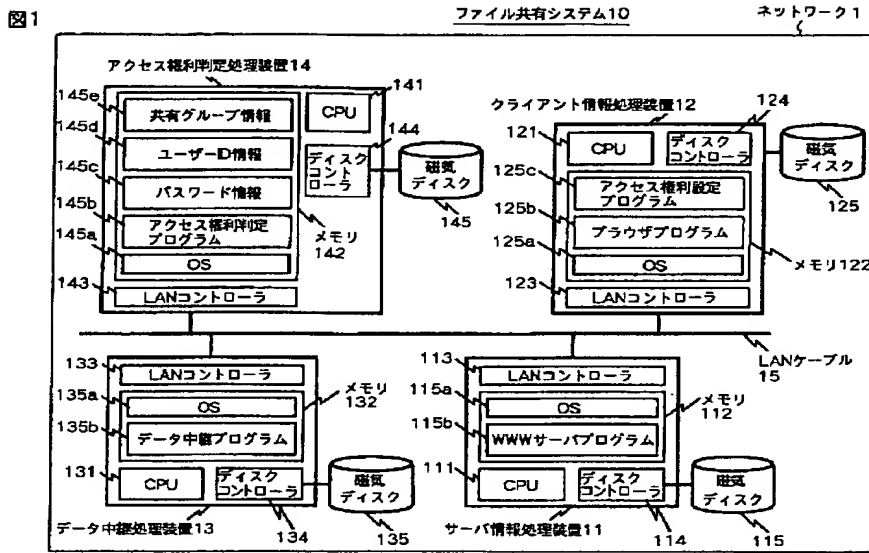
【図21】 アクセス権利が設定されたHTMLファイルを、アクセスする権利を持たないユーザーが閲覧しようとする場合に表示される、画面の一例である。

【図22】 アクセス権利が設定されたHTMLファイルを、アクセスする権利を持たないユーザーが閲覧する場合に表示される、エラーメッセージファイルの一例である。

【符号の説明】

1…ネットワーク、10…ファイル共有システム、11…サーバ情報処理装置、12…クライアント情報処理装置、13…データ中継処理装置、14…アクセス権利判定処理装置、111…CPU（中央演算処理装置）、112…メモリ、113…LANコントローラ、114…ディスクコントローラ、115…磁気ディスク、115a…OS（オペレーティングシステム）、115b…WWWサーバプログラム、121…CPU（中央演算処理装置）、122…メモリ、123…LANコントローラ、124…ディスクコントローラ、125…磁気ディスク、125a…OS（オペレーティングシステム）、125b…ブラウザプログラム、125c…アクセス権利設定プログラム、131…CPU（中央演算処理装置）、132…メモリ、133…LANコントローラ、134…ディスクコントローラ、135…磁気ディスク、135a…OS（オペレーティングシステム）、135b…データ中継処理プログラム、141…CPU（中央演算処理装置）、142…メモリ、143…LANコントローラ、144…ディスクコントローラ、145…磁気ディスク、145a…OS（オペレーティングシステム）、145b…アクセス権利判定プログラム、145c…パスワード情報、145d…ユーザーID情報、145e…共有グループ情報、200…ログイン証明書、300…HTMLファイル、400…アクセス権利が設定されたHTMLファイル、410…アクセス制御ヘッダ。

【図1】



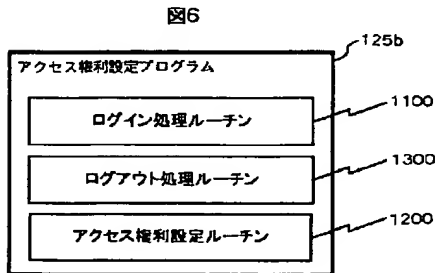
【図2】

図2

図2は、ID情報145dの表を示す。

カテゴリ	データ	コード
1 生年月日	19900101	-
2 氏名	榎号次郎	-
3 性別	男性	1
4 氏名コード	677991234	-
5 事業所	システム研究所	676
6 部	第四部	04
7 課	安全課	402
8 職名	主任	5
9 分野	セキュリティ	X5
10 出身地	神奈川	24

【図6】



【図3】

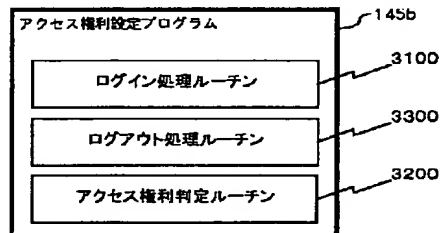
図3

図3は、グループ名と共有グループ情報の表を示す。

グループ名	共有グループ情報	作成者	作成日時
本社資材	5C=001^6C=11	001111234	1997.3.21
大阪資材	5C=101^6C=11	101115678	1997.3.21
本社営業	5C=001^6C=21	001210123	1997.4.1
大阪営業	5C=101^6C=21	101214567	1997.4.1
福岡営業	5C=103^6C=21	103218901	1997.4.1
西日本営業	0G=大阪営業,0G=福岡営業	001210001	1997.4.1

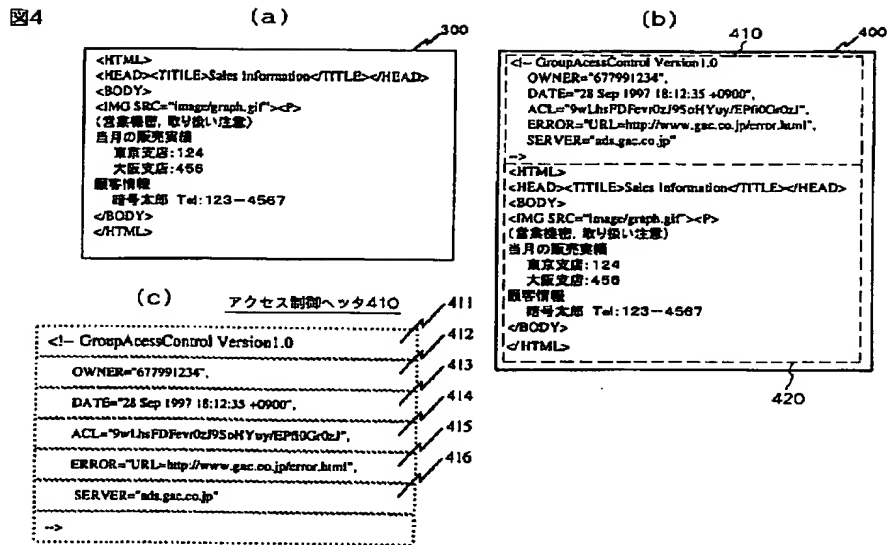
【図7】

図7



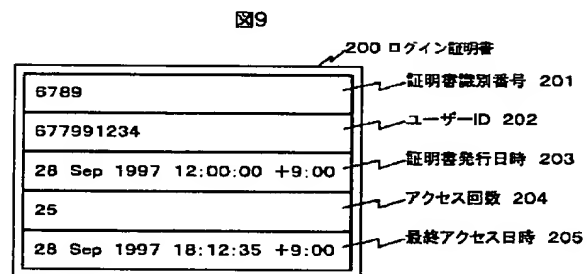
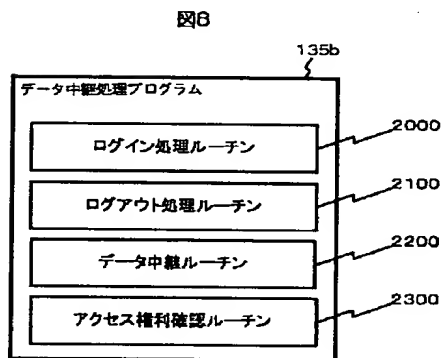


【図4】



【図8】

【図9】



【図11】

【図15】

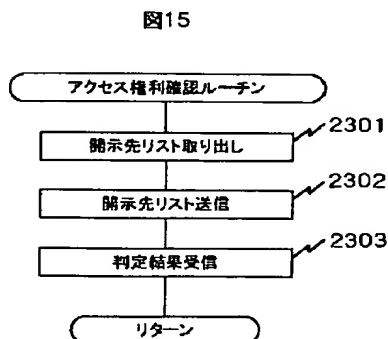
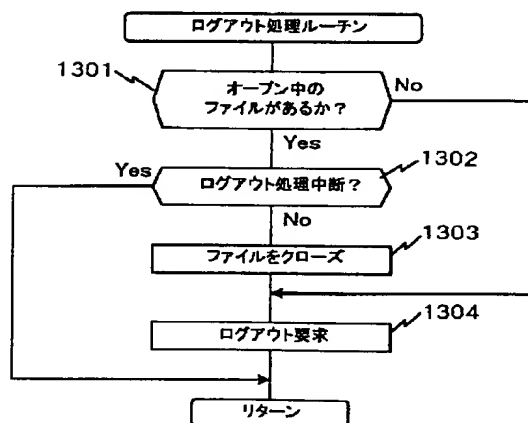
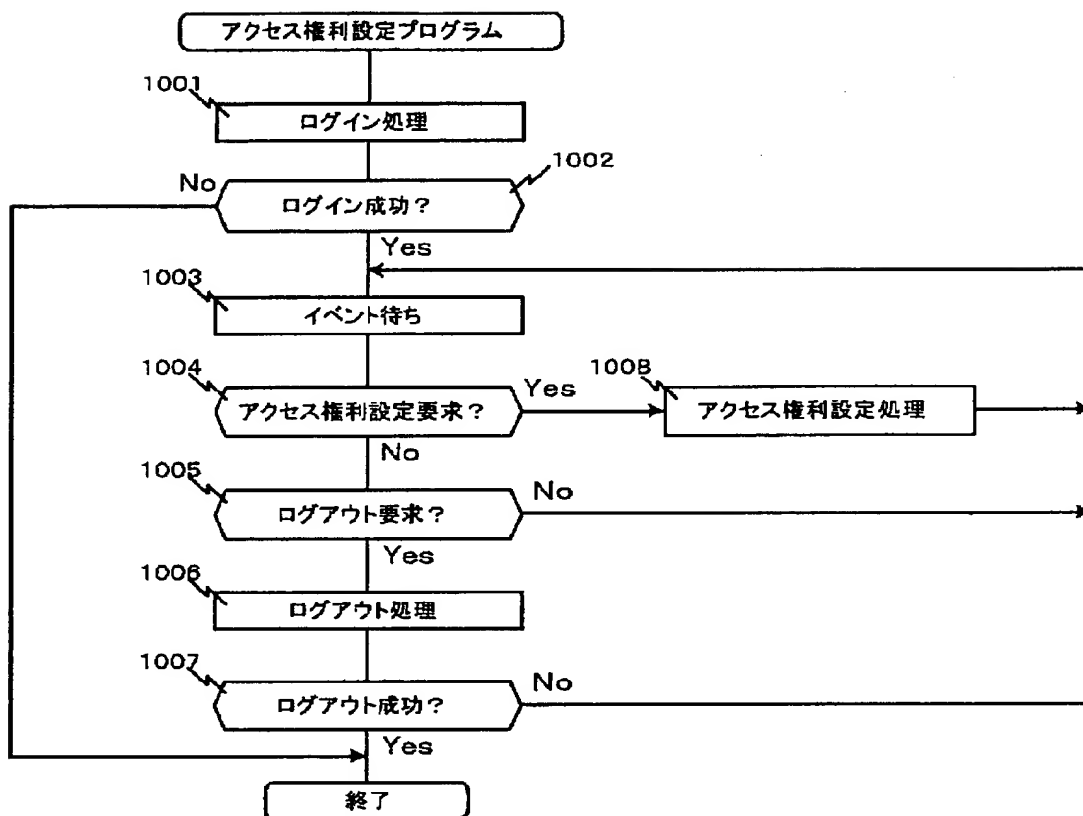


図11



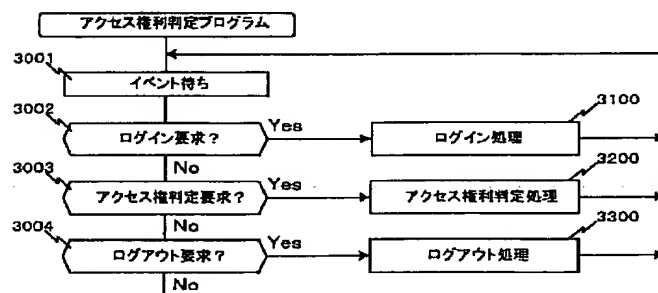
【図5】

図5



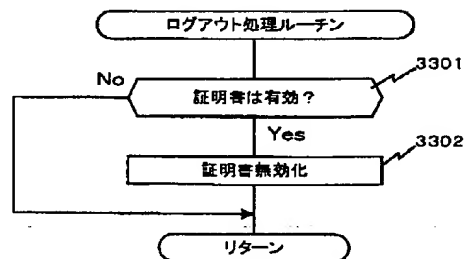
【図16】

図16



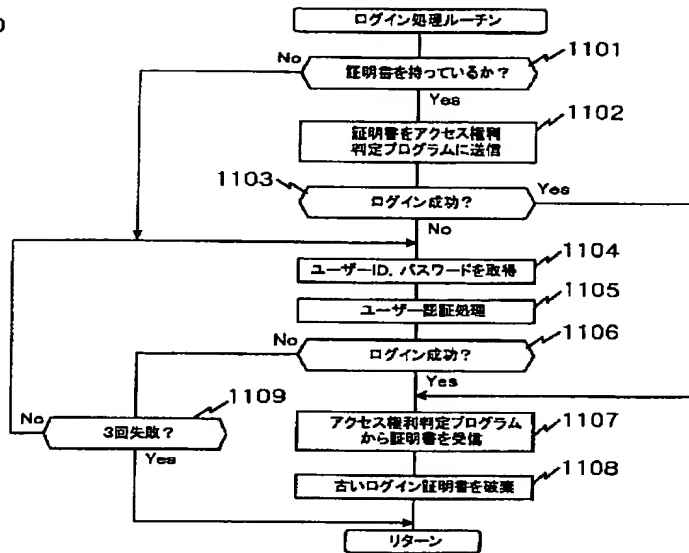
【図19】

図19



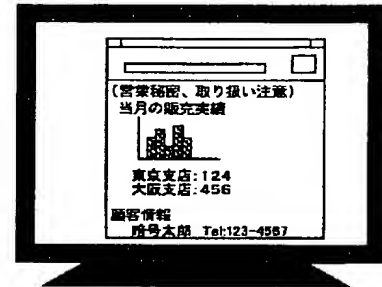
【図10】

図10



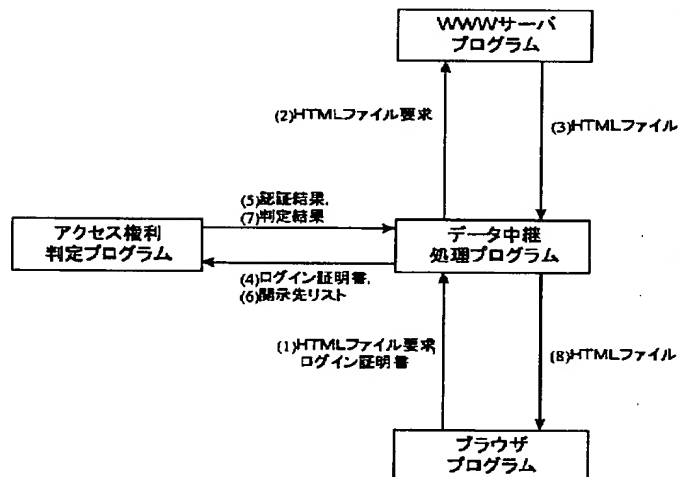
【図20】

図20



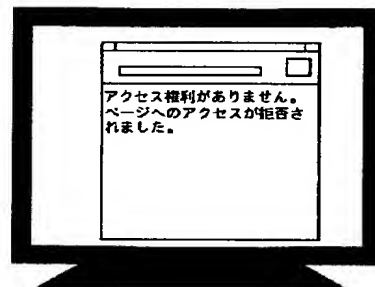
【図13】

図13



【図21】

図21



【図22】

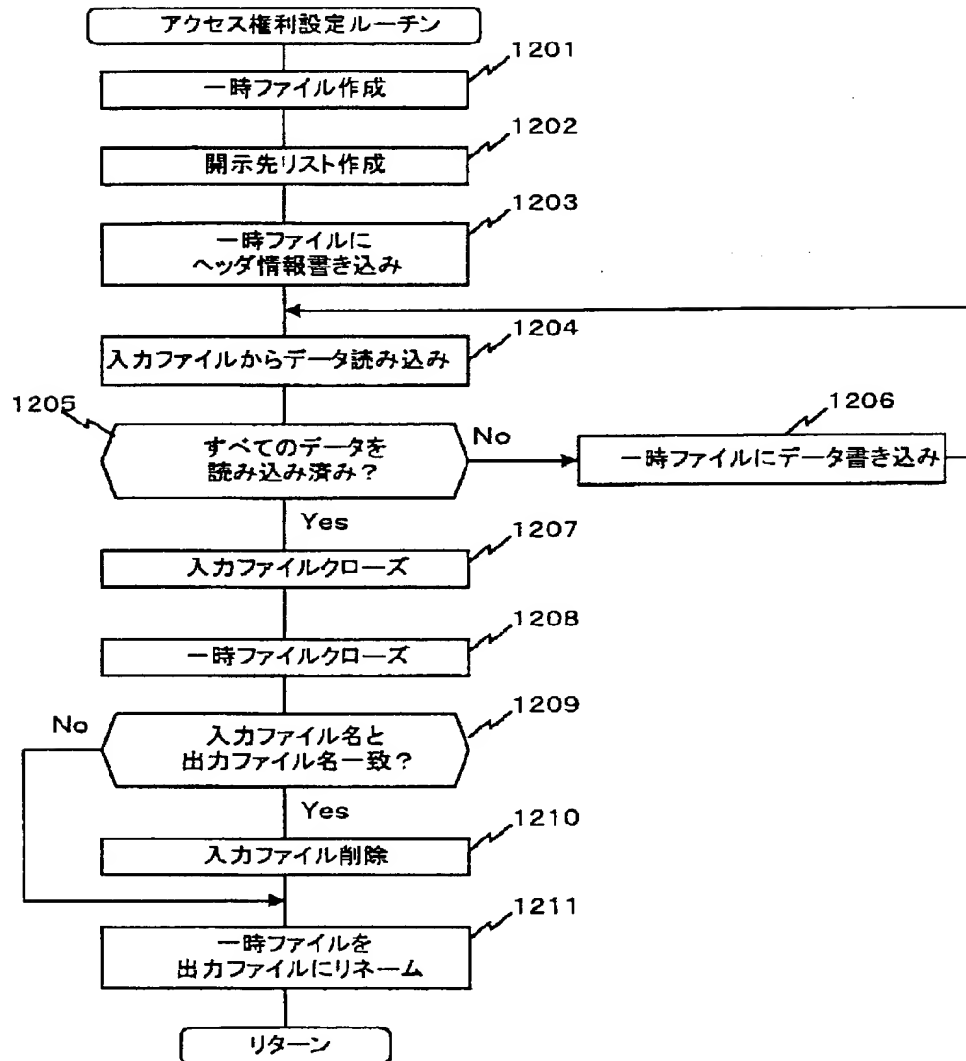
図22

```

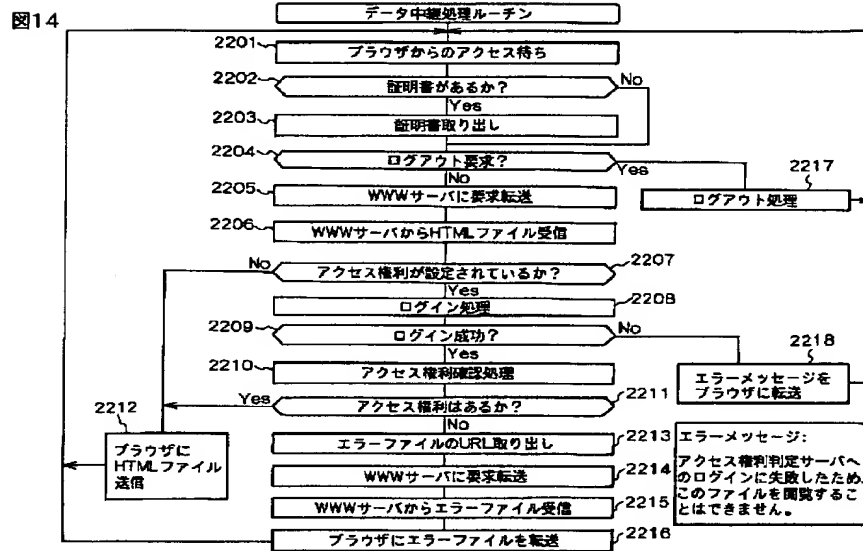
<HTML>
<HEAD><TITLE>Access Denied</TITLE></HEAD>
<BODY>
アクセス権がありません。
ページへのアクセスが拒否されました。
</BODY>
</HTML>
  
```

【図12】

図12

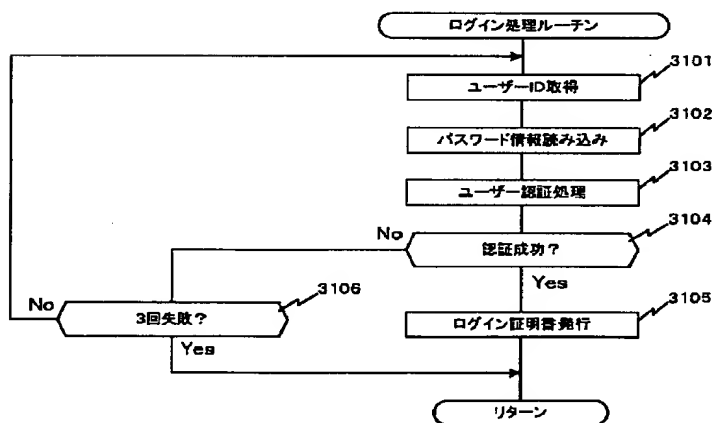


【図14】



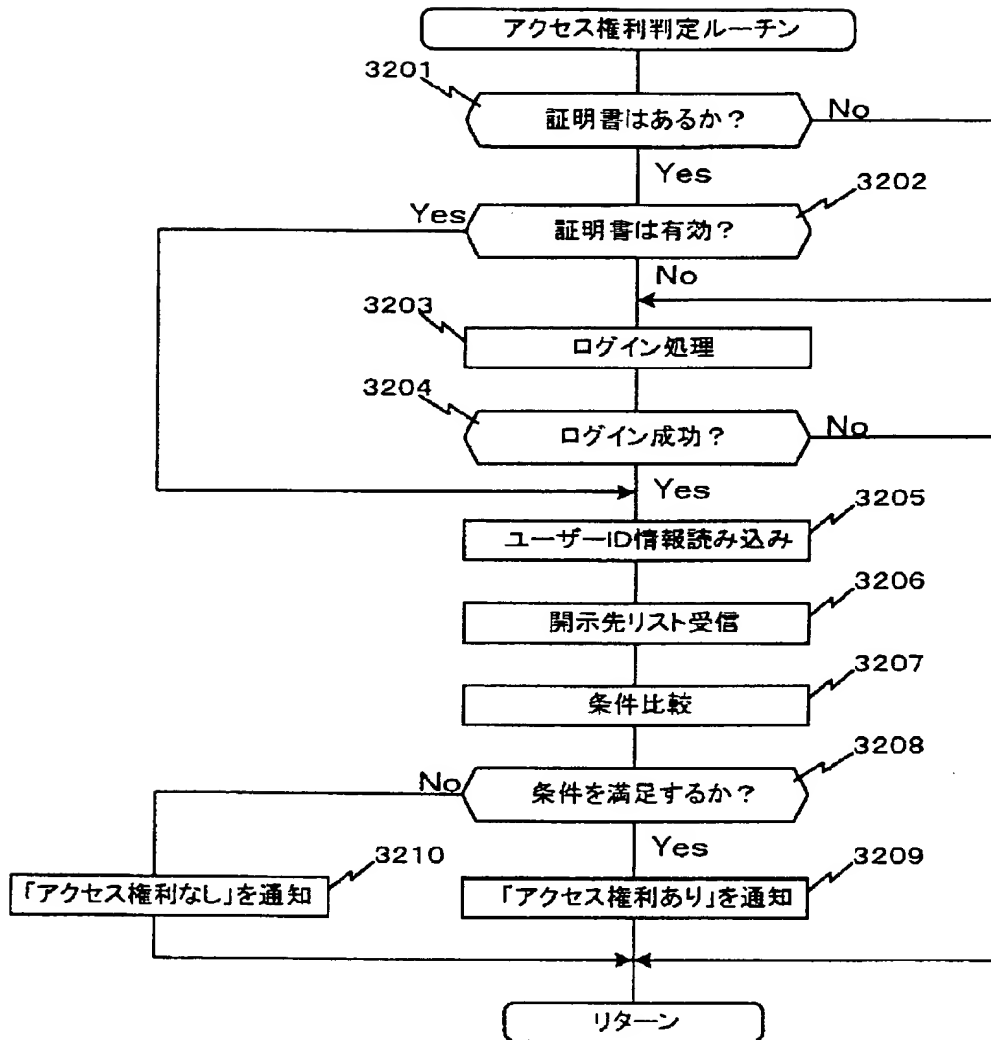
【図17】

図17



【図18】

図18



フロントページの続き

(72)発明者 柴田 利幸  
東京都品川区南大井六丁目26番3号 株式  
会社日立情報ネットワーク内

(72)発明者 今村 友彦  
東京都品川区南大井六丁目26番3号 株式  
会社日立情報ネットワーク内